PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	09/426,442	Confirmation No.: 1897
Appellant(s):	Sharyn Marie Garrity et al.	
Filed:	October 25, 1999	
Art Unit:	2134	
Examiner:	Christopher J. Brown	
Title:	SYSTEMS AND METHODS FOR SECURING EXTRANET TRANSACTIONS	

Docket No.: 99-703RCE1
Customer No.: 32127

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 CFR § 41.37

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed April 24, 2006.

Table of Contents.

1. ***Real Party in Interest.***

The real party in interest in this appeal is Verizon Corporate Services Group, Inc., an affiliate of Verizon Communications Inc.

2. ***Related Appeals and Interferences.***

There are no related appeals and/or interferences involving this application or its subject matter.

3. ***Status of Claims.***

Claims 1-17 are pending, all of which stand rejected and are being appealed.

4. ***Status of Amendments.***

There are no un-entered amendments in this application.

5. ***Summary of Claimed Subject Matter.***

Embodiments of the present invention relate to systems and methods for providing secure access and transactions using an extranet. Generally, embodiments of the present invention control a user's access to resources of an extranet based upon privileges allotted to the respective user and based on the user's identity as confirmed by certificate authentication. Pat. Appl., page 6, lines 21-23. More particularly, embodiments of the present invention control access to an extranet based upon privileges allotted to a user such that the respective user may access certain portions of the extranet, while restricting the respective user from accessing certain other portions of the extranet. The present invention may, for example, permit a customer user to access marketing information and retail pricing information, but restrict the respective customer user from accessing wholesale pricing information or engineering schematic information. *Id.* at page 9, lines 10-12. Similarly, the present invention may, for example, permit a reseller user to access marketing information and wholesale pricing information, but restrict the respective reseller user from accessing engineering schematic information. *Id.* at page 9, lines 12-15.

The access system for a computer site of the claimed invention includes a certificate authentication component for verifying a user's identity from a digital certificate supplied by the user. This component may comprise, for example, a certificate authentication server 262 (*see* Figure 2), a hosting service 380 (*see* Figure 3) or a security application of a web server. *Id.* at page 12, lines 10-12; page 15, lines 19-22; and page 16, lines 5-6 and 16-17. As recited, the claimed system also includes a directory, coupled to the certificate authentication component, to maintain an account for each individual user, where each account includes an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access. This directory may be implemented, for example, by a directory server 242 (see Figure 2), a LDAP (Lightweight, Directory Access Protocol) directory server 342 or the aforementioned security application of a web server. *Id.* at page 11, lines 17-19; page 13, lines 5-8; page 15, lines 19-22; and page 16, lines 14-16. The claimed system further includes an access control system, coupled to the directory, for controlling access to a computer site based on the access policy associated with the individual user in a directory. In this regard, the access control subsystem may permit the user to access a portion of the

computer site and restrict the user from accessing one or more other portions of the computer site. This access control subsystem may comprise, for example, an access control policy server 260, 360 (see Figures 2, 3) or the aforementioned security application of a web server. *Id.* at page 11, lines 20-23; page 12, lines 8-10; page 15, lines 19-22; and page 16, lines 14-16.

As explained in the patent application on page 18, lines 12-21, embodiments of the present invention offers a number of advantages. In this regard, the use of digital certificates for authentication of user identities may permit strong protection of access to the extranet and to management functions. Also, the system may permit finely tuned access to portions of an extranet by a plurality of users.

Appellants further note that Claims 13-17 of the present application provide an access system comprising a number of means-plus-function elements as permitted by 35 U.S.C. § 112, sixth paragraph. As recited in independent Claim 13, the means for verifying a user's identity, means for maintaining an account for each individual user, and means for controlling access to a computer site may correspond to the aforementioned certificate authentication component, directory, and access control system, respectively. As recited in dependent Claim 15, the means for issuing digital certificates may correspond to certificate authority, which may comprise, for example, a certificate authority server 250 (see Figure 2) or the aforementioned security application of a web server. *See id.* at page 11, lines 15-16; page 12, lines 17-22; and page 15, lines 19-22. As recited by dependent Claims 16, the means for recording the user's actions may correspond to a log system, which may comprise, for example, the aforementioned security application of a web server. *See id.* at page 13, line 14 – page 14, line 3. And as recited by dependent Claim 17, the means for storing verified records may correspond to a transaction authentication system, which may also comprise, for example, the aforementioned security application of a web server. *See id.*

6. ***Grounds of Rejection to be Reviewed on Appeal.***

Currently, pending Claims 1-17 stand rejected under 35 U.S.C. § 103(a). In particular, the pending Claims 1, 2 and 7-14 stand rejected as being obvious over U.S. Patent No. 6,367,009 to Davis, et al. in view of U.S. Patent No. 5,948,064 to Bertram, et al. Pending Claims 4-6, 16 and 17 stand rejected as being obvious over Davis in view of Bertram, and in further view of U.S. Patent No. 6,240,091 to Philip Ginzboorg, et al. And pending Claims 3 and 15 stand rejected as being obvious over Davis in view of Bertram, and in further view of U.S. Patent No. 5,774,552 to Francine G. Grimmer.

7. ***Argument.***

As explained below, Appellants respectfully submit that Claims 1-17 are patentably distinct from Davis in view of Bertram, alone or further in view of Ginzboorg or Grimmer. Accordingly, Appellants respectfully request that the aformentioned rejections be reversed. All of the rejections are premised upon a combination of Davis and Bertram. As described below, however, Appellants respectfully submit that one skilled in the art would not be motivated to combine Davis and Bertram.

Davis discloses a system and method for extending the Secure Sockets Layer (SSL) security protocol to delegate authority and authentication from a client to a server (middle-tier server – MTS) for the server to establish a secure connection to a back-end application (end-tier server – ETS) on behalf of the client. As disclosed, a client may connect to a MTS to request/retrieve services of the MTS. To provide those services, however, the MTS may be required to request/retrieve information from an ETS. Davis, col. 9, lines 24-48. To provide the services and information in a secure manner, according to one embodiment, the client establishes a first secure session with the MTS via the exchange of certificates, including a client certificate and a MTS certificate. After establishing the first secure session, the client provides the MTS with a delegate certificate for authenticating to an ETS. In this regard, after the first session is established, the MTS establishes a second session with the ETS via another exchange of certificates. Instead of exchanging the MTS certificate for the ETS certificate, however, the MTS exchanges the client and delegate certificates for the ETS certificate. The ETS can thereafter establish a certificate chain to authenticate the client via the MTS. And if the ETS controls access to the information requested by the client, the ETS may consult an access control list (ACL) to determine if the client is authorized to retrieve the respective information. And if the client is authorized, the ETS fulfills the request; otherwise, the ETS rejects the request.

Bertram discloses a system and method for discovery of authentication server domains in a computer network. As disclosed, a client "discovers" various server domains by issuing requests to one or more of the servers in a network. The client then characterizes responses from discovered domains as being from a native or non-native server, and compiles a list of each such server type. These lists include the discovered domains as locations that can be chosen as targets

for client authentication requests. Accordingly, the client can initiate access to a discovered domain by issuing a client authentication request to the respective domain, which can authenticate the client against a user account for the client user. As also disclosed by Bertram, a client user may have a user account, such as a Windows NT user account, on selected server domain systems. The user account may include username, password, and some representation of privileges of the user.

Independent Claim 1 recites an access system for a computer site. As recited, the system includes a certificate authentication component to verify a user's identity from a digital certificate supplied by the user. The system also includes a directory, coupled to the certificate authentication component, for maintaining an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access. And the system further includes an access control system, coupled to the directory, for controlling access to a computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory.

In contrast to independent Claim 1, and as conceded by the final Official Action, Davis does not teach or suggest a directory maintaining an account for each individual user, where each account includes an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access. Also in contrast to independent Claim 1, and as further conceded by the Official Action, Davis does not teach or suggest controlling access to a computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory. Nonetheless, the final Official Action alleges that Bertram discloses these features, and that one skilled in the art would have been motivated to modify Davis to include the respective features, and thereby disclose the claimed invention. As motivation, the Official Action alleges that ACL's such as those of Davis do not provide the level of security and flexibility that user accounts do. And as further alleged in the Advisory Action, "one of ordinary skill in the art would understand that a user account with

access policies would be beneficial over a strict yes or no ACL." Advisory Action of March 15, 2006, page 2. Appellants respectfully disagree, and as explained below, respectfully submit that not only does the final Official Action fail to establish a proper motivation for combining Davis and Bertram, but that one skilled in the art would not have been motivated to modify Davis with the teachings of Bertram, as alleged.

A. Official Action fails to Establish Proper Motivation to Combine Davis and Bertram

In order to properly combine references, a teaching or motivation to combine the references is essential. *In re Fine*, 337 F.2d 1071, 1075 (Fed. Cir. 1988). And as stated in MPEP, "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." MPEP § 2143.01 (citing *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990)) (emphasis added). In fact, the Court of Appeals for the Federal Circuit has stated that, "[c]ombining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability -- the essence of hindsight." *In re Dembiczak*, 175 F.3d 994 (Fed. Cir. 1999). Although the evidence of a suggestion, teaching, or motivation to combine the references commonly comes from the prior art references themselves, the suggestion, teaching, or motivation can come from the knowledge of one of ordinary skill in the art or the nature of the problem to be solved. *Id.* In any event, the showing must be clear and particular and "[b]road conclusory statements regarding the teaching effect of multiple references, standing alone, are not 'evidence'." *Id.*

In this instance, Appellants respectfully submit that merely asserting that the level and flexibility of the security provided by Davis can be changed by modifying that system to include user accounts as disclosed by Bertram, without explaining the desirability of such a modification, does not by itself provide the requisite motivation or suggestion to combine the references. First, the Official Action does not allege any benefit to user accounts over ACL's, but merely that user accounts and ACL's provide different levels of security and flexibility. Even if the Official Action did suggest that those differences rendered user accounts more desirable than ACL's,

however, Appellants respectfully submit that the Official Action has not provided any objective evidence to support this suggestion, whether in the nature of the problem to be solved, any of the cited references, or knowledge of those skilled in the art.

Moreover, Appellants respectfully submit that without an express motivation provided in the cited references, merely suggesting that a first means for performing a function has different characteristics from a second means does not support an assertion that it would have been obvious to modify a system by replacing the second means with the first means, without explaining the desirability of such a modification to the system. For example, the mere assertion that Fort Knox has a higher level of security than a simple combination lock does not support a finding that it would have been obvious to modify the front door of one's apartment by replacing an existing combination lock with the security of Fort Knox. One must consider the nature of the problem to be solved in considering whether it would have been desirable for one skilled in the art to make such a modification (without an explicit motivation in the cited references). MPEP § 2143.01 I., *citing In re Kotzab*, 217 F.3d 1365, 1370 (Fed. Cir. 2000) ("The test for an implicit [motivation] is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art."). In the above example, an individual looking to secure their apartment in an efficient manner may not find it desirable to replace their combination lock with the security of Fort Knox, even though Fort Knox provides a higher level of security than the combination lock. And in the instant case, Appellants respectfully submit that one skilled in the art would not have been motivated to replace the ACL of the Davis system with the user accounts of the Bertram system, even if the ACL and user accounts provide different levels of security and flexibility.

Appellants therefore respectfully submit that the Official Action has failed to establish a proper motivation for modifying Davis with the teachings of Bertram and, therefore, has failed to establish proper motivation to combine Davis and Bertram.

B. No Motivation to Combine Davis and Bertram - Additional Reasons

Not only has the Official Action failed to establish a proper motivation for modifying Davis with the teachings of Bertram, Appellants respectfully submit that one skilled in the art

would not have been motivated to modify Davis with the teachings of Davis. Initially, Appellants note that, even if one skilled in the art would understand that a user account with access policies would be beneficial over a strict yes or no ACL, as alleged by the Advisory Action, Appellants respectfully submit that nowhere does Davis teach or suggest that its ACL is of a "strict yes or no" type. In fact, other than describing comparison of the user's name to a list of authorized users, Davis does not teach or suggest any particular properties of the respective list. As will be appreciated by those skilled in the art, an ACL may specify a set of permissions (e.g., read, write, delete, etc.) for a particular user.

Generally, ACL's such as those of Davis differ from user accounts such as those of Bertram in the entities to which they refer. In this regard, an ACL such as that of Davis is associated with an object such as a computer file, and typically includes at least a list of users authorized to access the respective object. Consistent with the disclosure of Davis, an ACL is consulted to determine if the user is authorized to retrieve information of the ETS. In contrast, a user account such as that of Bertram is associated with a user, and typically includes a username, password, and other information pertaining to that particular user. Thus, consistent with the disclosure of Bertram, a user may establish a user account for authenticating and identifying oneself to a server domain. Nowhere, however, does Bertram teach or suggest a user account providing any benefit to access control for the requested information of Davis over that already provided by the associated ACL. That is, for accessing a particular piece of information, as disclosed by Davis, nowhere does Bertram teach or suggest a user account providing any benefit over the ACL already provided by Davis. One could argue the differences between ACL's and user accounts, but nothing in Davis, Bertram or information generally known to those skilled in the art teaches or suggests the desirability of replacing one with the other for accessing the requested information of Davis, as alleged by the Official Action.

As further evidence that one skilled in the art would not have been led to the alleged combination, consider that Bertram (with its disclosed user accounts) predates, and is in fact assigned to the same entity as, Davis. Thus, if one skilled in the art would have found it desirable to employ user accounts (as in Bertram) instead of an ACL (as in Davis), Appellants

respectfully submit that the later Davis system has initially included such user accounts. As the inventors of the Davis system themselves chose to employ an ACL instead of user accounts, it stands to reason that in at least the context of the Davis system, it would not have been obvious to one skilled in the art to alter the ACL of the Davis system with user accounts, as in Bertram.

Thus, independent Claim 1 is not taught or suggested by Davis in combination with Bertram. The other independent claims, namely Claims 8 and 13, include comparable recitations to independent Claim 1 and are therefore patentably distinct from Davis and Bertram for at least the same reasons as described above in conjunction with independent Claim 1. The tertiary references likewise fail to cure the deficiencies of Davis and Bertram with the tertiary references only being cited by the Official Action in conjunction with features set forth in various dependent claims.

For each of the foregoing reasons, Appellants submit that the rejections of independent Claims 1, 8 and 13 should be reversed. Since the dependent claims include each of the recitations of a respective independent claim, Appellants submit that the rejections of the dependent claims should also be reversed for at least the same reasons as described above in conjunction with a respective independent claim.

CONCLUSION

For at least the foregoing reasons, Appellants respectfully request that the rejections be reversed.

Respectfully submitted,

Andrew T. Spence
Registration No. 45,699

CUSTOMER NO. 32127
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON AUGUST 21, 2006.

LEGAL02/30036203v1

8. ***Claims Appendix.***

The claims currently on appeal are as follows:

1. (Previously Presented) An access system for a computer site, comprising

a certificate authentication component to verify a user's identity from a digital certificate supplied by the user,

a directory, coupled to the certificate authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, and

an access control system, coupled to the directory, for controlling access to a computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory.

2. (Original) An access system as in claim 1, wherein the access policy includes information representative of a portion of the computer site to which the user is permitted access.

3. (Original) An access system as in claim 1, further comprising

a certificate authority component, coupled to the certificate authentication component, to issue digital certificates to the user.

4. (Original) An access system as in claim 1, further comprising

a log system, coupled to the certificate authentication component, to record the user's actions in the computer site.

5. (Original) An access system as in claim 1, further comprising

a transaction authentication system, coupled to the certificate authentication component, to provide verified records of transactions performed using the computer site.

6. (Original) An access system as in claim 5, wherein the transaction authentication system includes a digital signing module for validating transactions.

7. (Original) An access system as in claim 1, wherein the computer site is an extranet.

8. (Previously Presented) A method of regulating access to a computer site, comprising receiving from a user a request to access a computer site or a portion thereof, receiving information representative of the user's identity,

consulting a directory containing an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, to determine whether the user is permitted to access the computer site or portion thereof, and

controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy for the individual user.

9. (Original) A method as in claim 8, wherein consulting a directory includes checking the access policy to determine a portion of the compute site to which the user is permitted access.

10. (Original) A method as in claim 9, wherein the receiving a request includes receiving a URL address for a site within the computer site.

11. (Original) A method as in claim 8, wherein receiving information representative of the user's identity includes receiving a password, a retinal scan, a fingerprint, or a document capable of being decrypted by a public key.

12. (Original) A method as in claim 8, wherein receiving information representative of the user's identity includes receiving a digital certificate.

13. (Previously Presented) An access system for a computer site, comprising means for verifying a user's identity from a digital certificate supplied by the user,

means, coupled to the means for verifying a user's identity, for maintaining an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, and

means, coupled to the means for storing information, for controlling access to a computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in the means for storing information.

14. (Original) A access system as in claim 13, wherein the means for storing information includes information representative of a portion of the computer site to which the user is permitted access.

15. (Original) An access system as in claim 13, further comprising

means, coupled is said means for verifying a user's identity, for issuing digital certificates to the user.

16. (Original) An access system as in claim 13, further comprising

means, coupled to said means for restricting access, for recording the user's actions in the computer site.

17. (Original) An access system as in claim 13, further comprising

means, coupled to said means for verifying a user's identity, for storing verified records of transactions performed using the computer site.

9. ***Evidence Appendix.***

None.

10. ***Related Proceedings Appendix.***

None.